

CLAIMS

What is claimed is:

1. A method for facilitating secure hardware token issuance and use, comprising:
5 storing an only instance of a private key on the hardware token, the hardware token
being adapted to prevent the private key from being exported from the hardware token;
 binding the private key to a subscriber with a digital certificate;
 creating a contract establishing ownership over the physical manifestation of the
private key;
10 using the private key to create a digital signature on the hardware token.
2. The method of claim 1, wherein the hardware token is issued by a trusted entity.
3. The method of claim 2, wherein the contract specifies that the physical manifestation
15 of the private key is owned by the trusted entity.
4. The method of claim 3, wherein the trusted entity is an issuing participant.
5. The method of claim 1, wherein the contract specifies that the physical manifestation
20 of the private key is owned by a root entity.
6. The method of claim 1, wherein the contract specifies that the physical manifestation
of the private key is owned by the subscriber.
- 25 7. The method of claim 1, wherein the hardware token is a smartcard.
8. The method of claim 1, wherein the hardware token is a PCMCIA device.
9. The method of claim 1, wherein the private key is an identity private key.
- 30 10. The method of claim 1, wherein the hardware token comprises means for
monotonically counting each time the private key is used to create a digital signature.
11. The method of claim 1, wherein the hardware token comprises means for
35 permanently storing a PIN/passphrase.

12. The method of claim 11, wherein the subscriber must enter the PIN/passphrase before a digital signature is generated.

13. The system of claim 12, wherein the subscriber must enter PIN/passphrase each time
5 a digital signature is generated.

14. The system of claim 1, wherein the digital signature comprises security data.

15. The system of claim 14, wherein the security data is signed to create a security-data
10 cryptogram.

16. The system of claim 15, wherein the security-data cryptogram is generated using an algorithm different than the one used to create the digital signature.

15 17. The system of claim 14, wherein the security data comprises data that is the subject of the digital signature.

18. A method for facilitating secure smartcard issuance and use, comprising:
providing a smartcard;
20 generating a private key on a hardware security module not resident on the smartcard;
copying the private key into memory on the smartcard;
adapting the smartcard to prevent the private key from being exported from the smartcard; and
25 destroying all instances of the private key not resident in the memory on the smartcard.

19. A system for facilitating secure smartcard issuance and use, comprising:
a smartcard;
30 means for generating a private key on a hardware security module not resident on the smartcard;
means for copying the private key into memory on the smartcard;
means on the smartcard for preventing the private key from being exported from the smartcard; and

35

means for destroying all instances of the private key not resident in the memory on the smartcard.

20. A method for facilitating secure hardware token issuance and use, comprising:

- 5 providing a signing module, the signing module comprising a hardware token, the hardware token permanently storing a single instance of a private key and being adapted to sign data in connection with transactions conducted within the context of a four-corner model comprising a root entity, a first participant, a second participant, a first customer of the first participant, the first customer having possession of the hardware token, and a
10 second customer of the second participant;
the root entity identifying a plurality of high-level security objectives relating to the hardware token, the high-level security objectives comprising:
 - a. It is beyond practicality to breach the confidentiality of the private key;
 - b. It is beyond practicality to breach the confidentiality of a PIN/passphrase
15 stored on the hardware token;
 - c. It is beyond practicality to change the life-cycle status of the hardware token;
 - d. It is beyond practicality to breach the integrity of the counters associated with blocking and unblocking mechanisms on the hardware token;
 - e. It requires a high security level attack to breach the confidentiality and/or
20 integrity of data and program structures on the hardware token;
 - f. It requires a high security level attack to breach the integrity of a bond between the first customer's identity and the hardware token;
 - g. It requires a high security level attack to breach the integrity of root entity applications present at the hardware token; and
 - 25 h. It requires a high security level attack to breach the integrity of the signing module; and
the root entity identifying a plurality of low-level requirements to address the high-level objectives.

30 21. The method of claim 20, wherein the low-level requirements comprise:

- a. It is beyond practicality to remove layers on top of a chip surface of the hardware token without damaging the chip;
- b. It requires a high security level attack to visualize the contents of read only memory (ROM) memory cells, including electrically erasable programmable read only
35 memory (EEPROM) cells;

- c. It is beyond practicality to reverse engineer the functionality of the hardware token;
- d. It is beyond practicality to modify chip structures by means of an FIB system;
- 5 e. It is beyond practicality to modify individual memory cells;
- f. It requires a high security level of attack to misuse the hardware token chip's test features;
- g. It requires a high-level security attack to modify the hardware token chip's fuses;
- 10 h. It requires a high-level security attack to modify or disable hardware token chip 401's security sensors;
- i. It is beyond practicality to use a probing attack to retrieve information from the hardware token;
- j. It requires a high security level attack to change the status of a memory of the
- 15 hardware token via active probing techniques;
- k. It requires a high security level attack to influence the correct functionality of logical building blocks at the hardware token by means of active probing techniques;
- l. It requires a high security level attack to influence the correct execution of applications approved by the root entity at the hardware token by means of active probing
- 20 techniques;
- m. It requires a high security level attack to influence the correct programming of memory cells by means of active probing attacks;
- n. It requires a high security level attack to obtain information from the hardware token via voltage contrast;
- 25 o. It is beyond practicality to obtain sensitive information from the hardware token by analyzing externally available information, such as a power consumption profile or timing analysis of critical processes on the hardware token;
- p. It is beyond practicality to influence the correct execution of applications approved by the root entity on the hardware token by disturbing external parameters such as
- 30 clock input, temperature, or power supply;
- q. It is beyond practicality to obtain sensitive information by disturbing external parameters of the hardware;
- r. It requires a high security level attack to change the status of the memory by means of disturbing external parameters of the hardware token.

35

22. The method of claim 21, further comprising identifying a plurality of potential threats to the hardware token and determining that the low-level requirements address the potential threats.

5 23. The method of claim 22, wherein the potential threats comprise chip modification, reverse engineering, restoration of testing hardware and software, internal attack, and external attack.

24. The method of claim 23, wherein the external attacks include SPA, DPA, and
10 manipulation of the hardware token environment.

15

20

25

30

35